ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/309292171

Cognitive Electronic Warfare System

Conference Paper · October 2016

DOI: 10.13140/RG.2.2.10939.62240

CITATIONS
5

READS
16,517

1 author:

Ameer Sameer
University of Babylon

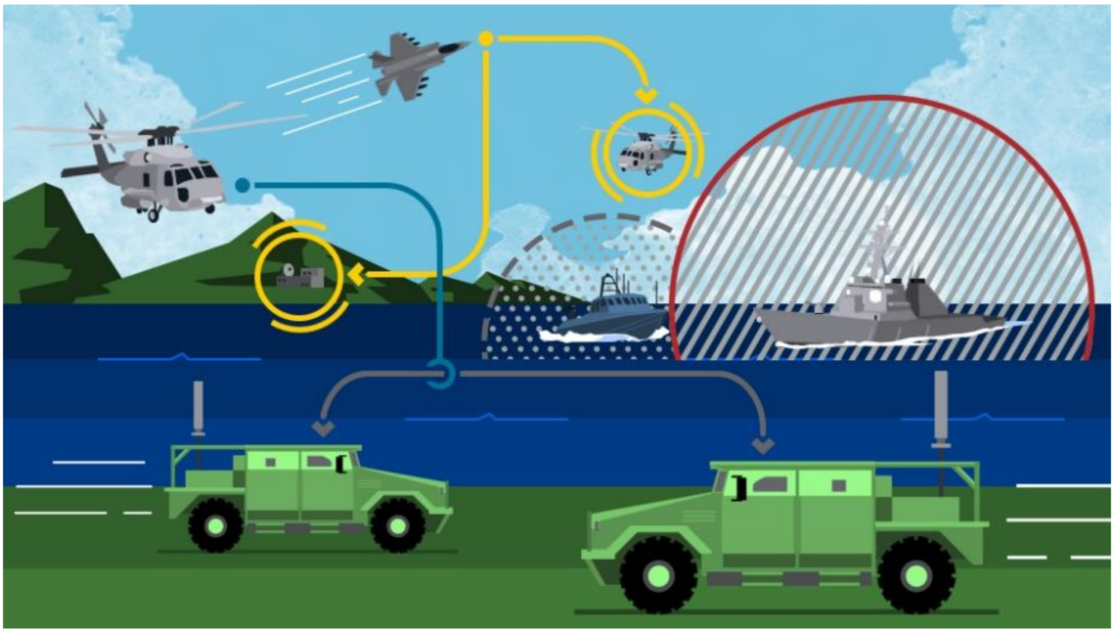
46 PUBLICATIONS **47** CITATIONS

SEE PROFILE

All content following this page was uploaded by Ameer Sameer on 20 October 2016.

The user has requested enhancement of the downloaded file.

Cognitive Electronic Warfare System



Prepared by: Ameer Sameer Hamood

University of Babylon - Iraq

Information Technology - Information Networks

﴿ بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ ﴾

اقْرَأْ بِاسْمِ رَبِّكَ الَّذِي خَلَقَ ﴿١﴾ خَلَقَ الْإِنسَانَ مِنْ عَلَقٍ ﴿٢﴾ اقْرَأْ وَرَبُّكَ الْأَكْرَمُ ﴿٣﴾ الَّذِي
عَلَّمَ بِالْقَلَمِ ﴿٤﴾ عَلَّمَ الْإِنسَانَ مَا لَمْ يَعْلَمْ ﴿٥﴾

﴿ In the Name of Allah, the Merciful, the Most Merciful ﴾

Read (Prophet Muhammad) in the Name of your Lord who created,﴿١﴾ created the human from a (blood) clot. ﴿٢﴾Read! Your Lord is the Most Generous, ﴿٣﴾ who taught by the pen, ﴿٤﴾ taught the human what he did not know. ﴿٥﴾

Table of contents

Introduction to cognitive electronic warfare ١

Adaptive Radar Countermeasures (ARC) ....

Behavioral Learning for Adaptive Electronic Warfare (BLADE) ....

Types of Electronic Warfare ....

Handheld cognitive electronic warfare 2

Cognitive networked electronic warfare 3

DARPA XG Cognitive Radio 4

Realtime Cognitive Electronic Warfare 5

Electronic warfare (EW)

Electronic warfare uses focused energy, usually radio waves or laser light, to confuse or disable an enemy's electronics. It can also involve listening —collecting an enemy's radio signals or sensing the radar of an incoming missile.

Raytheon has been a leader in electronic warfare since World War II, when it developed a magnetron, or radio wave generator, that became a key part of the Allies' radar systems. In recent years it has pioneered the use of gallium nitride, a substance that produces five times more radio energy than previous technologies.

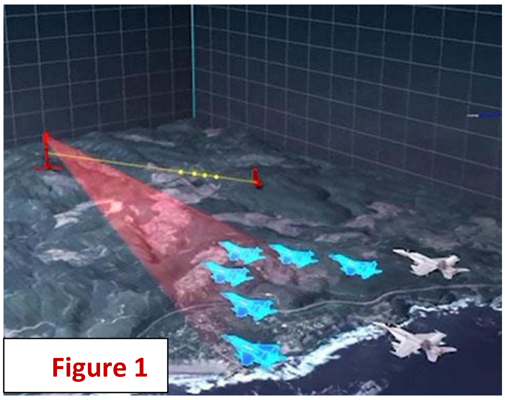


Figure 1

Today the company is developing tactical lasers, the Next Generation Jammer and other weapons, along with electrical systems capable of powering whatever innovations the future holds.

Through a contract from the Defense Advanced Research Projects Agency (DARPA), BAE Systems has developed a new handheld tactical sensor designed to enhance soldiers' understanding of radio frequency (RF) signals for improved situational awareness.

Figure 2

By using cognitive processing algorithms, this electronic warfare (EW) technology can quickly detect and identify multiple interfering signals, such as jammers or enemy communication signals, across a wide spectrum and in changing and challenging environments.

The new capability is designed to be leveraged across multiple platforms and can integrate, for example, into a variety of EW, SIGINT and signal receiver and communication systems.

“By drastically reducing the size, weight, and power of this new cognitive EW system, we're making it easier for our warfighters to be aware of, classify and manage a wide range of signals in the battlespace, which is crucial for tactical situational awareness," said Joshua Niedzwiecki, director of sensor processing and exploitation at BAE Systems. "Better situational awareness on the battlefield means superior protection for our troops and a greater ability to defeat hostile threats."

The technology was developed under DARPA's Computational Leverage Against Surveillance Systems (CLASS) program and the Cognitive radio Low-energy signal Analysis Sensor ICs (CLASIC) program. The goal was to improve on today's portable spectrum analyzers, which are often bulky, power hungry and unable to handle interference or classify the signals they detect.

Using advanced signal processing algorithms, BAE Systems states that it was able to reduce the time and computing power needed to process detected signals to such an extent that the new system uses only one low-power chip. The result is an order of magnitude reduction in size, weight and power compared to conventional spectrum analyzers.

During recent field tests, the new technology successfully detected and identified more than 10 signal types across a wide bandwidth in the presence of interference. The company expects to continue to mature this technology for eventual deployment within its EW, SIGINT, and tactical communications portfolios.

Types of Electronic Warfare

There are three basic types of electronic warfare:

- passive Electronic Support Measures (ESM)
- active Electronic CounterMeasures (ECM)
- anti-ECM Electronic Counter-CounterMeasures (ECCM)

One of the problems with the last two types is the continuous development of one equipment to counter the other. As the ECM specialist produces systems to provide jamming and decoy methods so the ECCM engineer develops equipment to overcome these methods. Frequently the same manufacturers are doing both!

The electronic warfare scene is a continuously evolving battle between the various aspects of ESM, ECM and ECCM. With the complexity of modern weapons, and the speed of reaction necessary to combat them, the weak link in the chain would appear to be the human being who has to make the decision! This is not necessarily the case, because in some instances an operator is far better than an automatic processor. He can interpret situations based on previous experience more readily and can alter his thresholds easily to perform basic functions such as detecting a signal in heavy background clutter, whereas a machine can only operate at the threshold for which it has been programmed. Nevertheless, great strides have been made in artificial intelligence systems and, although there is still a long way to go, the era of complete automation will eventually arrive. The amount of raw information from modern sensor systems is so vast that better and better processors, employing highly complex software programs, are vital to analyse the inputs. This speed and complexity is such that the operators must be highly efficient, and an extensive business in providing EW training and simulation systems has grown up over the past years. Even so, this does not help, say the pilot of a single-seat fighter who is being presented with a vast amount of electronic information and, perhaps, only a second or so to react against a missile attack. All that this means, in that type of situation, is that the warning system must be fully automatic in its countermeasures role, with an overriding manual facility as a safety measure.

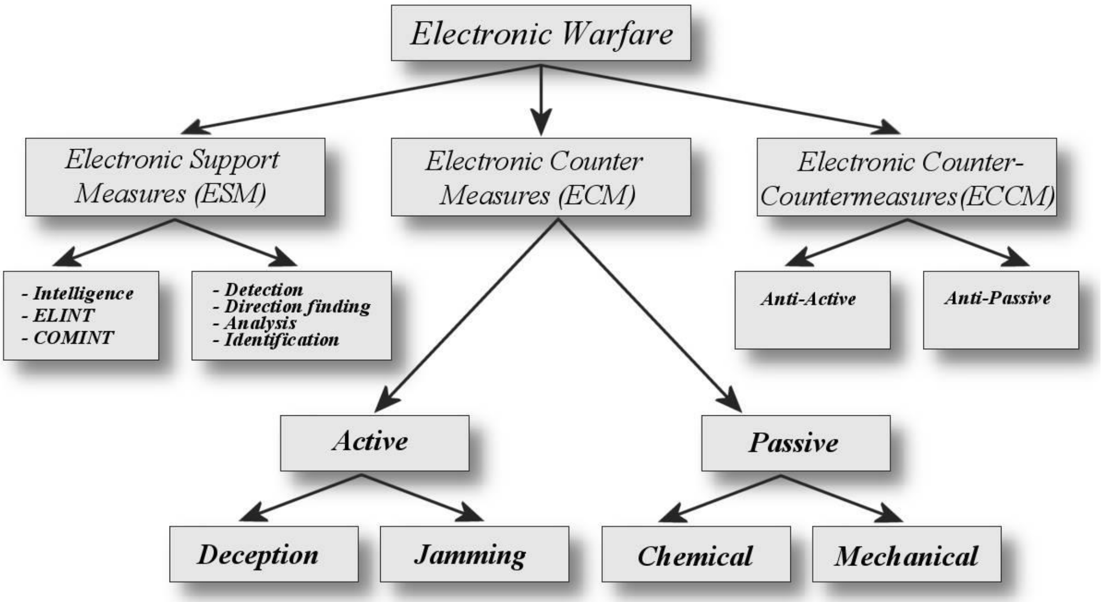


Figure 3: Elements of Electronic Warfare

Another vital component is the provision of programmable software so that the system program can be changed easily. It is interesting to note that EW systems used in the Gulf War were designed to cope with Soviet missiles and radars but, in some cases, found themselves faced with Western systems. Fortunately the most up-to-date radar warning receivers and jammers are software controlled and were able to be reprogrammed to meet the threats.

Cognitive Radio as the Facilitator for Advanced Communications Electronic Warfare Solutions

Throughout the 1990s, Software Defined Radio (SDR) technology was viewed almost exclusively as a solution for interoperability problems between various military standards, waveforms and devices. In the meantime, Cognitive Radio (CR) – a novel communication paradigm which embodies SDR with intelligence and self-reconfigurability properties – has emerged. Intelligence and on-the-fly self-reconfiguration abilities of CRs constitute an important next step in the Communications Electronic Warfare, as they may enable the jamming entities with the capabilities of devising and deploying advanced jamming tactics. Similarly, they may also aid the development of the advanced intelligent self-reconfigurable systems for jamming mitigation.

This work outlines the development and implementation of the Spectrum Intelligence algorithm for Radio Frequency (RF) interference mitigation. The developed system is built upon the ideas of obtaining relevant spectrum-related data by using wideband energy detectors, performing narrowband waveform identification, extracting the waveforms' parameters and properly classifying the waveforms. All relevant spectrum activities are continuously monitored and stored. Coupled with the self-reconfigurability of various transmission-related parameters, Spectrum Intelligence is the facilitator for the advanced interference mitigation strategies. The implementation is done on the Cognitive Radio test bed architecture which consists of two military Software Defined Radio terminals, each interconnected with the computationally powerful System-on-Module.

Adaptive Radar Countermeasures (ARC)

Figure 4

Current airborne electronic warfare (EW) systems must first identify a threat radar to determine the appropriate preprogrammed electronic countermeasure (ECM) technique. This approach loses effectiveness as radars evolve from fixed analog systems to programmable digital variants with unknown behaviors and agile waveforms. Future radars will likely present an even greater challenge as they will be capable of sensing the environment and adapting transmissions and signal processing to maximize performance and mitigate interference effects.

The goal of the Adaptive Radar Countermeasures (ARC) program is to enable U.S. airborne EW systems to automatically generate effective countermeasures against new, unknown and adaptive radars in real-time in the field. ARC technology will:

- Isolate unknown radar signals in the presence of other hostile, friendly and neutral signals.
- Deduce the threat posed by that radar.
- Synthesize and transmit countermeasure signals to achieve a desired effect on the threat radar.
- Assess the effectiveness of countermeasures based on over-the-air observable threat behaviors.

ARC technologies will be developed using an open architecture to allow for insertion, modification and removal of software modules with minimal effect on other elements of the system. ARC algorithms and signal processing software will be suitable both for new EW systems and for retrofitting into existing EW systems without extensive rework of front-end radio frequency hardware.

Behavioral Learning for Adaptive Electronic Warfare (BLADE)

The Behavioral Learning for Adaptive Electronic Warfare (BLADE) program is developing the capability to counter new and dynamic wireless communication threats in tactical environments. BLADE is enabling a shift from today's manual-intensive lab-based countermeasure development approach to an adaptive, in-the-field systems approach. The program will achieve this by developing novel-machine learning algorithms and techniques that can rapidly detect and characterize new radio threats, dynamically synthesize new countermeasures, and provide accurate battle damage assessment based on over-the-air observable changes in the threat.

Handheld cognitive electronic warfare

Lightweight, handheld tactical sensor that soldiers can easily carry and use to better understand radio frequency (RF) signals for enhanced situational awareness. By using cognitive processing algorithms, this system can quickly detect and identify multiple interfering signals, such as jammers

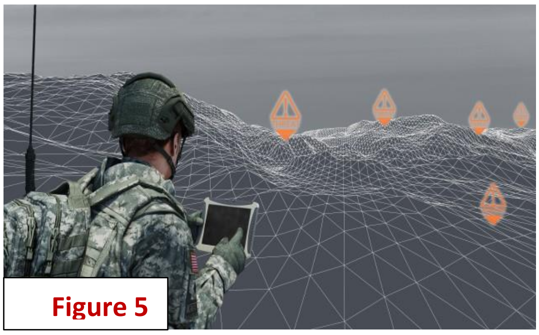


Figure 5

or enemy communication signals, across a wide spectrum and in changing and challenging environments. Developed under DARPA’s Computational Leverage Against Surveillance Systems (CLASS) program.

An apparatus for sensing and classifying radio communications is provided. The apparatus includes one or more sensor units configured to detect radio frequency signals, a signal classifier configured to classify the detected radio frequency signals into a classification, the classification including at least one known signal type and an unknown signal type, a clustering learning algorithm capable of finding clusters of common signals among the previously seen unknown signals. The system is then further configured to use these clusters to retrain the signal classifier to recognize these signals as a neW signal type.

Sensing the use of radio frequencies, identifying the users, and potentially jamming their future use are becoming increasingly important in many fields. Such Radio Frequency (RF) sensing and jamming techniques are being used in mili tary applications, laW enforcement, and commercial applica tions. Military applications include Electronic Warfare (EW), such as (a) Electronic Situation AWareness (ESA) (e.g., map ping all the RF signals present in a given region), (b) Electronic Attack (EA) (e.g., (i) deactivation of IEDs and (ii) jamming enemy communications), and (c) Electronic Protection (EP) (e. g., identifying friendly communication being jammed and protecting it from being j ammed by changing the frequency). Just RF sensing alone can also be used for many military applications, such as eavesdropping on enemy communication, Signal Intelligence (SIGINT) and Communication Intelligence (COMINT). LaW enforcement applications may include disrupting communications of criminals in drug raids and terrorists, and dealing With ho stage situations. Commercial applications may include prevention of corporate espionage.

Several systems have been developed for RF EW and some commercial products are available. These systems are based on energy detectors, maximum likelihood based classifiers, and a signal generator that jams the identified source. However, conventional systems are unable to automatically adapt to the environmental conditions, cannot handle signals that are unknown to the system, and are developed for the detection and classification of only certain broad classes of RF signals. Furthermore, conventional systems often have limited adaptation capability, Which if available, is typically handled by manual adjustment. These systems are able to collect data When they encounter signals that the system is not trained for. HoWever, such data is unusable until the systems are retrained in the laboratory and redeployed. Such a process takes months. By then neW signals/threats may appear in the field of operations.

In vieW of the foregoing, the present disclosure presents an automatically adaptable Cognitive NetWorked (collaborative) Electronic Warfare (CNEW) System. The disclosed system includes a cognitive scheduler that consists of an event based cognitive controller, service management layer, and netWork management. The cognitive controller consists of learning, optimiZation, reasoning and verification, and validation engines. These engines learn, adapt and control the functionalities and parameters of the sensor, detector, signal classifier (including specific emitter identification (SEI)),jammer, radio netWork and geo-location unit. The disclosed system improves the RF signal detection accuracy in fading environments by collaborative sensing and improves the jamming range and reduces collateral damage

(a) by determining the locations of the objects such as hills,foliage or Walls that can block the detectors and jamming signals and (b) by calculating strategic locations for the sensor and jammer nodes to avoid these blockages. Furthermore,the system manages communication of friendly netWorks so that the “blue” forces alWays maintain spectral dominance. In all these applications, the disclosed system improves performance as it is adaptable and has the capability to accurately detect/classify/geo-locate different types of signals (a priori knoWn/unknoWn) in varied environments. According to one embodiment of the disclosure, an apparatus for cognitive netWorked electronic Warfare is provided. Among numerous functionalities, the apparatus may include functionality for ESA and EA. Such an apparatus includes one or more sensor units configured to detect radio frequency signals, a signal classifier configured to classify the detected radio frequency signals into a classification, the classification including a knoWn signal type and an unknoWn signal type, a clustering learning unit configured to determine a model of common feature values from data relating to radio frequency signals classified as an unknoWn signal type, the common set of feature values being used to generate a neW known signal type, a cognitive controller configured to initiate the clustering learning unit When the signal classifier classifies a detected radio frequency signal as an unknoWn signal type, the cognitive controller being further configured to re-train the signal classifier With the neW knoWn signal type When the clustering learning unit generates the neW knoWn signal type. In additional embodiments of the disclosure, the apparatus may further include a cognitive controller configured to initiate a policy engine to determine Whether the classified signal is an enemy signal and make a decision as to attack it. The cognitive controller initiates the jammer and jammer optimization engine if the decision is to attack. The jammer optimization engine is configured to optimiZe the jamming parameters and to synthesiZe and transmit the jamming signal to attack the enemy.

DARPA XG Cognitive Radio

In a most general sense, cognitive radio takes advantage of Moore’s law to capitalize on the computational power of semiconductor industry. When information is accessible in digital domain, the force driver behind this novel radio is computationally intelligent algorithms. Machine learning and artificial intelligence have become the new frontier toward this vision—analogy of robotics. Converting information from analog domain to digital domain plays a central role in this vision: revolutionary compressed sensing is, thus, critical to expanding the territory of this new system paradigm. The agile, software defined radios that can perform according to the algorithms are basic building blocks. When each node is computationally intelligent, wireless networking faces a novel revolution. In a system level, the functions such as cognitive radio, cognitive radar and anti-jamming (even electronic warfare) have no fundamental difference and are unified in a single framework that requires inter-disciplinary knowledge. Radar and communications should be unified since both require dynamic spectrum access—the bottleneck. Spectrum agile/cognitive radio is a new paradigm in wireless communications—a special application of the above general radio.

Spectrum agile/cognitive radio is a new paradigm in wireless communications, as illustrated by DARPA XG radio in Figure 6. Cognitive radios can opportunistically use spectrum white space and increase usage by ten times . One ingredient of this paper is to investigate a novel, wideband (multi-GHz) system architecture enabled by compressive sampling (or compressed sensing)—a revolutionary breakthrough in applied mathematics and signal processing. The other is to design multi-GHz spectrum sensing and experimental system testbeds. These ingredients share the same goal of bringing together three separate system paradigms: cognitive radio, cognitive radar, and electronic warfare. The Department of Defense (DoD) is transforming the military into a more responsive digitized force capable of of rapidly deploying and effectively operating in all types of military operations; an intensive information network becomes critical. Such an example is wireless sensor networks . A 2003 Congressional Budget Office report concluded: "current demand within the Army is larger than the supply by *an order of magnitude* and these shortfalls will continue into and after 2010 with shortage as high as *30 times* at some command levels." To solve this bandwidth shortage, improvements in spectrum usage are required. These bandwidth shortages are occurring even though a vast amount of the allocated spectrum is virtually unused or under-used. This paradox results from the current static and inefficient allocation process. In response, the Federal Communication Commission (FCC) and US DoD recently issued separate challenges to address the poor efficiency of static spectrum assignment in licensed bands.

A recent study conducted by Shared Spectrum shows that average spectrum occupancy in the frequency band from 300 MHz to 3000MHz over multiple locations is merely 5.2%. The maximum occupancy is about 13% in New York City . It can be found that the spectrum scarcity is mostly caused by the fixed assignment to the wireless service operators, and there exist spectrum opportunities both in spatially and temporally. Therefore, the interest in allowing access to unutilized spectrum by unlicensed user (second user) has been growing in several regulatory bodies and standardization groups, e.g. the FCC and IEEE 802.22—the first complete cognitive radio-based international standard . In particular, the spectrum scarcity is the most severe problem for US for wireless services, partially due to the fact that US has most dense spectrum usage. There is a common belief that we are running out of usable radio frequencies. Cognitive radio (CR) provides an alternative (a new paradigm) to systems such as the third generation (3G) and the fourth generation (4G). Due to the Department of Defense (DoD) focusing on the Joint Tactical Radio System (JTRS), US has a clear technical leadership in cognitive radio.

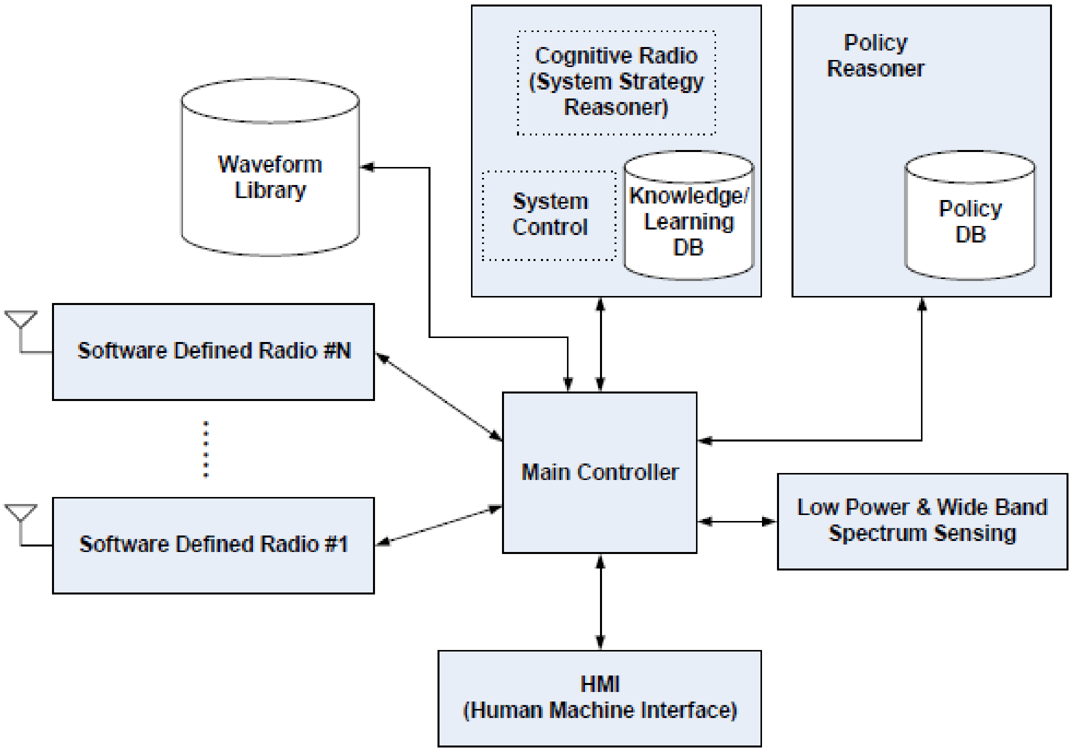

Waveform Library
Cognitive Radio (System Strategy Reasoner)
System Control
Knowledge/ Learning DB
Policy Reasoner
Policy DB
Software Defined Radio #N
Software Defined Radio #1
Main Controller
Low Power & Wide Band Spectrum Sensing
HMI (Human Machine Interface)

Figure 6: DARPA XG Cognitive Radio.

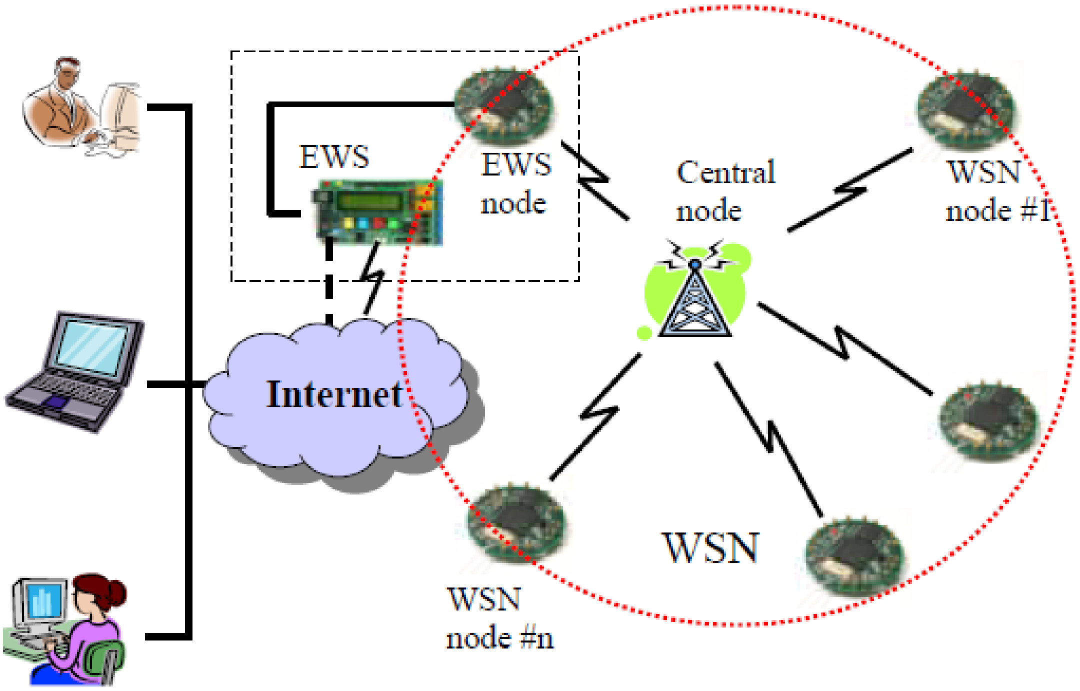


Figure 7: Embedded Web Server (EWS) for Wireless Sensor Networks (WSN).

Realtime Cognitive Electronic Warfare

DARPA applying Artificial Intelligence for realtime cognitive electronic warfare modern radar and communications systems can subtly and quickly change their character, making them harder for U.S. aircraft and other platforms to jam or spoof. That reality is prompting DARPA to lead industry teams to apply artificial intelligence to electronic warfare. It's called "cognitive EW."

The difference between today's tech and that of the 1970s lies in the adoption of readily available digital processing. Such processing effectively allows operators to change aspects of the waveforms that radar and communications systems use. "The problem now is that if we continue to rely on that [old] approach, the radar waveforms we're expecting could be rapidly changed," Tilghman says. "Cognitive EW is being developed to deal with the unexpected."

DARPA's new approach uses machine learning algorithms to assess and characterize radar and communications emitters in real time. It learns their characteristics in the moment and then produces a countermeasure. It's not that the system is inventing new countermeasures on the fly. Rather, Tilghman says, cognitive EW "deduces the right set of countermeasures to employ." Of course, the secretive agency won't say how quickly the AI can assess and respond, only that the "time frame is sufficient to meet the needs of countering that radar."

This cognitive EW effort began in 2010 and is broken into two parts: Adaptive Radar Countermeasures (ARC) and Behavioral Learning for Adaptive Electronic Warfare (BLADE). The two tracks exist because of the differing nature of thwarting an enemy's radar and its communications.

References:

1- COGNITIVE NETWORKED ELECTRONIC WARFARE
Shubba L. Kadambe, Cedar Rapids, IA
(US); Benjamin J. Haan, Marion, IA
(US); Jason A. Fuemmeler, Cedar
Rapids, IA (US); W. Sam Spencer,
Cedar Rapids, IA (US); Carlos J.
Chavez, Marion, IA (US); Robert J.
Frank, Cedar Rapids, IA (US)

2- Exploiting Cyclostationarity for Radio Environmental Awareness in Cognitive Radios
3- Cognitive Radio Architecture
4- A Unified Framework for Cognitive Radio, Cognitive Radar, and Electronic Warfare— Tutorial, Theory, and Multi-GHz Wideband Testbed
5- A scalable dynamic spectrum allocation system with interference mitigation for teams of spectrally agile software defined radios
6- Evolution of spectrum-agile cognitive radios: first wireless internet standard and beyond
7- Embedded web server for wireless sensor networks
8- A Survey on Spectrum Management in Cognitive Radio Networks
9- Implementation issues in spectrum sensing for cognitive radio

https://www.researchgate.net/profile/Ameer_Sameer

https://www.linkedin.com/in/ameer-sameer-452693107

http://www.slideshare.net/AmeerSameer

http://facebook.com/ameer.Mee/

View publication stats